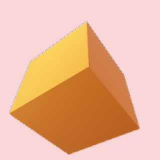
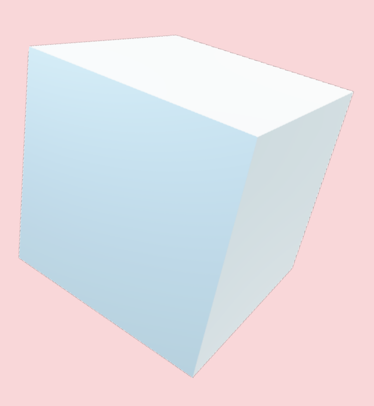

Axiom JDK Pro:
новые вызовы российской
Java-разработки
Олег Чирухин
HL++
HighLoad++
2022



Java 19





Надежный

и безопасный стек Java-технологий

Рантайм Java

Какой дистрибутив использовать?

AXIOM JDK PRO

Сервер приложений

Где запускать JavaEE/JakartaEE?

LIBERCAT

Контейнеры и облака

На каких образах запускать?

AXIOM RUNTIME CONTAINERS

Безопасность

Куда бежать с WebLogic?

AXIOM TRUSTED REPOSITORY

Таймлайн

От Java до OpenJDK и Axiom JDK

Почти 25 лет опыта разработки Java платформы

1995
Java1.0a2

Опыт инженеров БЕЛЛСОФТ в разработке Java платформы

1996
Java Development Kit (JDK) 1.0

1997
По контракту с Sun Microsystems



1998
Открыт стандарт Java
Java Community Process (JCP)

2004
Центр разработки в Санкт-Петербурге









2007
Создание проекта OpenJDK

OpenJDK

2010
Центр разработки в Санкт-Петербурге

ORACLE

2017
Oracle объявляет об изменениях лицензии Java и планах окончания поддержки Java 8

Создание компании БЕЛЛСОФТ

2018
100% исходного кода Java SE открыто в OpenJDK, включая коммерческий функционал

Выпуск российской платформы Java

2020
AXIOM JDK PRO

Платформа для карты «Мир», СБП, 1С, М.Видео

Развиваем OpenJDK

JEP 315: Improve Aarch64 Intrinsics

Owner	Dmitrij Pochepko
Type	Feature
Scope	Implementation
Status	Closed / Delivered
Release	11
Component	hotspot / compiler
Discussion	hotspot dash compiler dash dev at openjdk dot java dot net
Effort	L
Duration	L
Reviewed by	Mikael Vidstedt, Vladimir Kozlov
Endorsed by	Vladimir Kozlov
Created	2017/10/10 12:40
Updated	2018/09/10 14:45
Issue	8189104

Summary

Improve the existing string and array intrinsics, and implement new intrinsics for the `java.lang.Math` sin, cos and log functions, on AArch64 processors.

JEP 386: Alpine Linux Port

Owner	Boris Ulasevich
Type	Feature
Scope	Implementation
Status	Closed / Delivered
Release	16
Component	hotspot
Discussion	portola dash dev at openjdk dot java dot net
Effort	M
Duration	M
Reviewed by	Alan Bateman, Vladimir Kozlov
Endorsed by	Mikael Vidstedt
Created	2019/08/13 10:33
Updated	2021/08/28 00:30
Issue	8229469

Summary

Port the JDK to Alpine Linux, and to other Linux distributions that use musl as their primary C library, on both the x64 and AArch64 architectures,

JEP 388: Windows/AArch64 Port

Authors	Monica Beckwith, Ludovic Henry, Bernhard Urban-Forster
Owner	Vladimir Kozlov
Type	Feature
Scope	Implementation
Status	Closed / Delivered
Release	16
Component	hotspot
Discussion	aarch64 dash port dash dev at openjdk dot java dot net
Effort	M
Duration	S
Blocks	JEP 391: macOS/AArch64 Port
Reviewed by	Vladimir Kozlov
Endorsed by	Mark Reinhold, Vladimir Kozlov
Created	2020/06/29 19:13
Updated	2021/08/28 00:28
Issue	8248496

Summary

Port the JDK to Windows/AArch64.

JEP 391: macOS/AArch64 Port

Authors	Anton Kozlov, Vladimir Kempik
Owner	Vladimir Kempik
Type	Feature
Scope	JDK
Status	Closed / Delivered
Release	17
Component	hotspot
Discussion	aarch64 dash port dash dev at openjdk dot java dot net
Effort	M
Duration	M
Depends	JEP 388: Windows/AArch64 Port
Reviewed by	Andrew Haley, Vladimir Kozlov
Endorsed by	Vladimir Kozlov
Created	2020/08/07 07:08
Updated	2021/09/29 17:30
Issue	8251280

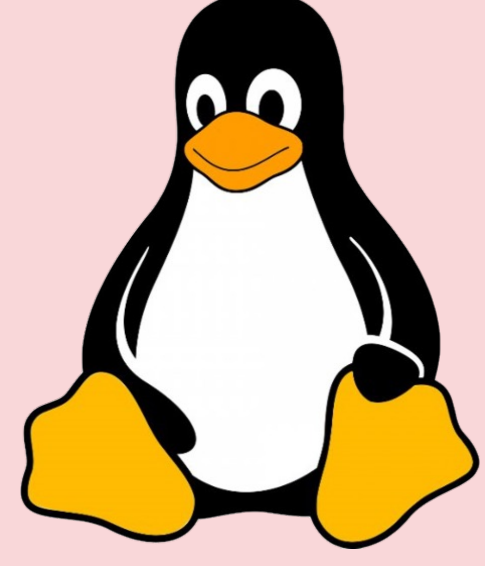
Summary

Port the JDK to macOS/AArch64.

Наш вклад
в Open source

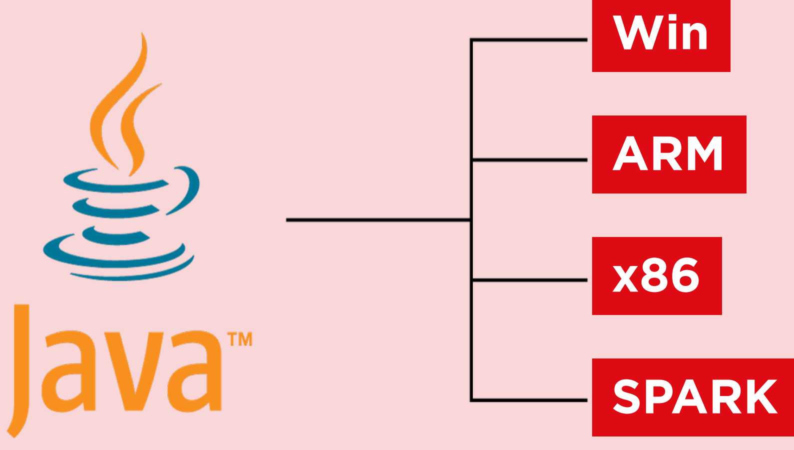












AXIOM JDK PRO

Российский Java Runtime

- Java: LTS (8, 11, 17), старые версии: 6,7
- Популярные процессоры и операционные системы
- Российские платформы: Байкал , Скиф, МЦСТ SPARC
- Российские ОС: Astra Linux, Alt Linux, РЕД ОС, РОСА
- Современные сборщики мусора: ZHC, Shenandoah, G1
- GUI и Web: OpenJFX, Applets, OpenWebStart
- ГОСТ Криптография, интегрированная с КриптоПРО JCP и КриптоПРО CSP, сертифицированная в ФСБ
- Собственные разработки | например, Axiom Administration Center

AXIOM JDK CERTIFIED

Средство защиты информации с сертификатом ФСТЭК УД4

- Независимость экземпляров виртуальных машин
- Верификация class-файлов
- Безопасное выполнение интерпретируемого кода
- Управление доступом
- Контроль целостности исполняемого кода
  замкнутая программная среда
- Регистрация событий безопасности
- Очистка памяти

AXIOM JDK CERTIFIED

Средство защиты информации с сертификатом ФСТЭК УД4

- **При создании государственных информационных систем до 1 класса защищенности включительно**
  в соответствии с документом «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденным приказом ФСТЭК России от 11 февраля 2013 г. № 17 с изменениями, внесенными приказом ФСТЭК России от 15 февраля 2017 г. № 27

- **В значимых объектах критической информационной инфраструктуры 1 категории**
  в соответствии с документом «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», утвержденным приказом ФСТЭК России от 25 декабря 2017 г. № 239

- **При создании информационных систем персональных данных до 1 уровня защищенности включительно**
  в соответствии с документом «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным приказом ФСТЭК России от 18 февраля 2013 г. № 21 с изменениями, внесенными приказом ФСТЭК России от 23 марта 2017 г. № 49

AXIOM NIK PRO

Инструментарий нативных образов

- Основан на GraalVM
- Компилирует Java-приложение в исполняемые exe-файлы
- Совместим с Alpine Linux
- Снижает размер базового образа и затраты на облака
- Позволяет писать микросервисы на разных языках
  JavaScript, LLVM, Python, Ruby, R, WebAssembly
- Поддерживает большинство популярных платформ
  Linux и Mac, glibc и musl, x86_64 и ARM64

JDK 16

- **JEP 386: Alpine Linux Port**
- **openjdk.java.net/jeps/386**
- **openjdk.java.net/projects/portola**
  Порт JDK на дистрибутив Alpine Linux, в частности, musl C library



Owner	Boris Ulasevich
Type	Feature
Scope	Implementation
Status	Integrated
Release	16
Component	hotspot / runtime
Discussion	portola dash dev at openjdk dot java dot net
Effort	M
Duration	M
Reviewed by	Alan Bateman, Vladimir Kozlov
Endorsed by	Mikael Vidstedt
Created	2019/08/13 10:33
Updated	2020/10/14 07:48
Issue	8229469

Summary

Port the JDK to Alpine Linux, and to other Linux distributions that use musl as their primary C library, on both the x64 and AArch64 architectures,

Motivation

Musl is an implementation, for Linux-based systems, of the standard library functionality described in the ISO C and POSIX standards. Several Linux distributions including Alpine Linux and OpenWrt are based on musl, while some others provide an optional musl package (e.g., Arch Linux).

The Alpine Linux distribution is widely adopted in cloud deployments, microservices, and container environments due to its small image size. A Docker base image for Alpine Linux, for example, is less than 6 MB. Enabling Java to run out-of-the-box in such settings will allow Tomcat, Jetty, Spring, and other popular frameworks to work in such environments natively.

By using `jlink` (JEP 282) to reduce the size of the Java runtime, a user will be able to create an even smaller image targeted to run a specific application. The set of modules required by an application can be determined via the `jdeps` command.



Axiom
Runtime Container Pro

- Самые легкие Java-контейнеры на рынке
- Первый Linux, оптимизированный для Java
- Основан на Alpine — стандарте облачной разработки
- CI/CD: Discovery API, Trusted Docker Registry, унифицированная среда
- Все инструменты в одном образе
- Коммерческая поддержка в России
- Слой совместимости musl с glibc | скорость + безопасность
- Собственный Trusted Docker Registry | не Docker Hub

Базовый образ

Linux для Axiom Runtime Container Pro

- **Ядро:**
  - Linux LTS
  - SecureBoot
  - Подписи модулей
  - Оптимизации

- **LIBC**: musl + glibc, несколько реализаций malloc
- **Пакеты**: Alpine Linux aports (APK)
- Поддержка **Docker**, QEMU
- **Оптимизации** для Axiom JDK Lite и Native Image Kit (NIK)

LIBERCAT

Российский сервер приложений

- Возможная альтернатива Oracle WebLogic, IBM WebSphere и др.
- Основан на TomEE Plus
- Реализует спецификации JavaEE/JakartaEE
- Подходят примеры из интернета и документация на Tomcat и JavaEE

Сервер приложений:

- Обработка HTTP
- Data persistence, ORM, Web Services
- Поддержка микросервисной архитектуры (MicroProfile, OpenTracing…)
- Множество дополнительных технологий (JMS, JAX-WS, JSF…)



Использует Axiom JDK Pro
вместо Oracle Java для КИИ

ПС «Мир» нагрузочные параметры

- Процессинг: 420 банков, 19+ млрд транзакций в год, 170+ банков-эмитентов, 145 млн карт выдано
- Клиринг: 20 млн финансовых сообщений в день
- Система лояльности: 29 млн карт, 22,4 млн клиентов
- 24/7, система высокой доступности SLA — 99,99





MirAccept

- Дополнительная защита онлайн-платежей на базе 3D Secure

СБП — Система Быстрых Платежей





5 млн операций в день

на Axiom JDK Pro, доверенной российской Java-платформе

Мгновенные межбанковские переводы без карты

- Использует каждый третий житель России
- 1 млрд операций в I полугодие 2022 (5 млн в день)
- 211 банков подключены
- 63+ млн уникальных пользователей



Оплата товаров и услуг по QR-коду, кнопке или ссылке

- 362 тысячи точек оплаты на предприятиях торговли и сервиса

Оптимизация микросервисов

Варианты проектов по оптимизации Java-стека



Альфа-Банк перенес разработку

мобильного банка на легковесные контейнеры Axiom Runtime Containers



М.Видео отметил ускорение разработки на 15%

при использовании легковесных контейнеров Axiom Runtime Containers. Это произошло за счет сокращения времени пулинга и редеплоя, экономии инженерного времени и дискового пространства. Свою роль сыграли Discovery API и Trusted Docker Registry для безопасной интеграции в CI/CD процесс

Open source:

уязвимости
и их исправление





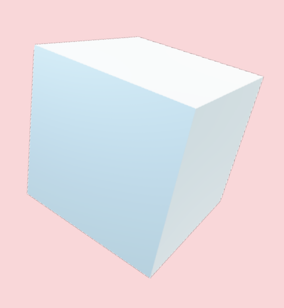


Баги

масштаб проблемы

Соотношение
СОЗДАННЫХ и РЕШЕННЫХ
задач в проекте JDK
за последние 7 200 дней

Протестное движение
и «отмена» России



- Удаление или порча файлов пользователей с IP из России и Беларуси. Пакеты peacenotwar (CVE-2022-23812), node-ipc (CVE-2022-23812) и т.п.
- Отображение текстовой и графической пропаганды на сайтах и при сборке: es5-ext, EventSource, Evolution CMS, AWS Terraform module и т.п.
- Удаление поддержки российских аппаратных платформ (Quake3e удалил поддержку Elbrus)
- Удаление русской локализации (RESP.app / RedisDesktopManager)
- Блокировка внешних ресурсов и репозиториев (pnpm)







Трагедия
Марака Сквайрса

- Известный и уважаемый разработчик
  - Colors.js — расцветка консоли Node.js
  - Faker.js — генератор случайных реалистичных данных
- Сгорела квартира, ожоги, личные проблемы
- Попытался получить финансирование в Forbes top-500
- Удалил репозиторий faker.js, добавил в начало кода библиотеки colors.js бесконечный цикл

Исправление уязвимостей

Log4Shell | CVE-2021-44228

- Уязвимость в log4j
- Атакующий с помощью параметров логгера может запустить произвольный код со своего LDAP сервера
- Команда Axiom JDK выпустила Live Patch

Psychic Signatures | CVE-2022-21449

- Уязвимость в OpenJDK
- Позволяет манипулировать подписями, например в TLS 1.3 может выдать произвольный сервер за доверенный
- Команда Axiom JDK выпустила обновление дистрибутива



Vulnerability workflow






Новая проблема

- Исследование
- Репорт
- Квалификация

Разбор и валидация

- Разбор отчета
- Тест POC
- CVSS score
- CVE ID
- JBS issue

Разработка патча

- POC
- Разработка
- Тесты
- Ревью

План

- Дата
- Бэкпорты

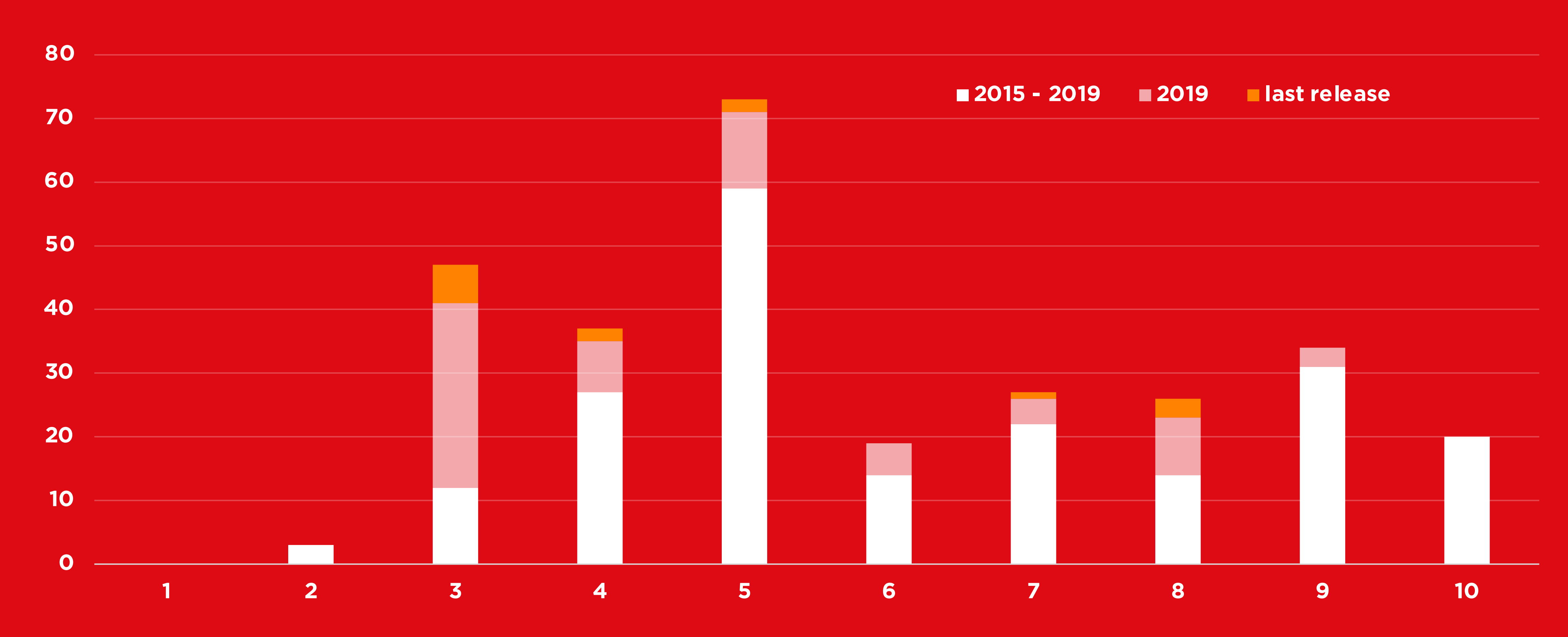


Публикация

- Раскрытие
- Патчи

Данные

по устраненным проблемам с безопасностью в Java



Статический анализ
и зависимости







Svace



Статический анализ:

- Более 100 тыс. срабатываний
- Стратегия обработки
  - Critical with Very High and High Availability
  - 98 срабатываний
- 26 дефектов исправлены в JDK 8
- 22 дефекта исправлены в JDK 11

- Перехват компиляции
  - Java
  - C/C++
  - Нужен исходный код
- Перехват сборки Maven/Ant

Регрессионные тесты

- **Jtreg** | https://openjdk.org/jtreg
- **Полный прогон тестов около 16 часов**

Санитайзеры

- **Санитайзеры для GNU Compiler Collection** | https://gcc.gnu.org
- **AddressSanitizer, ASan** | утечки памяти
- **UndefinedBehaviorSanitizer, UBSan**
  UB — самая большая проблема C++

Фаззинг
и тестовое покрытие



AFL++

A security-oriented fuzzer



JQF

Semantic Fuzzing for Java



Jazzer

Coverage-guided, in-process fuzzing for the JVM



LCOV

Покрытие C/C++



Jcov

Покрытие Java

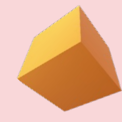
ФСТЭК СЗИ УД4

AXIOM JDK
CERTIFIED

- Государственные информационные системы **до 1 класса защищенности** включительно
- Значимые объекты критической информационной инфраструктуры **1 категории**
- Информационные системы персональных данных **до 1 уровня защищенности** включительно
- Автоматизированные системы управления производственными и технологическими процессами **1 класса защищенности**

Доверенный
репозиторий





- Axiom JDK Pro | основан на OpenJDK
- Libercat | основан на Tomcat / TomEE+
- Spring Framework
- Инструменты сборки | Maven, Ant, Gradle
- Другие стандартные библиотеки

Экосистема

российской Java: Axiom JDK































ROSA



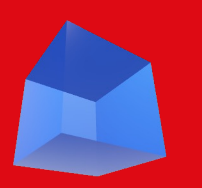







Надежный

и безопасный стек Java-технологий





Рантайм Java

AXIOM JDK PRO

Сервер приложений





Контейнеры и облака

AXIOM RUNTIME CONTAINERS

Безопасность

AXIOM TRUSTED REPOSITORY



AXIOM JDK

Спасибо

за внимание!




Олег
Чирухин
Директор по коммуникациям
в команде Axiom JDK
oleg@axiomjdk.ru

Обратная связь
и комментарии по
докладу по ссылке



